UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,493	07/05/2001	Amiram Ofir	OFIR2	8439

1444 7590 11/30/2004

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
ALOMARI, FIRAS B	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/898,493	OFIR, AMIRAM	
	Examiner	Art Unit	
	Firas Alomari	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *07/05/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DTEAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Baltzley (US. 6,154,543).

a. Regarding claim 1, Baltzley discloses a method for allowing a sender to send an encrypted message to at least one recipient from any data terminal connected to a data communication network and being capable of securely sending data to at least one computer connected to the data communication network (Abstract lines 11-12 and Col 2, lines 21-25), said method comprising:

- Providing a virtual network connectable to the data communications network (item 115 of FIG.3) and providing access to respective user space dedicated (Col 6, lines 23-26) to the sender and each recipient for storing a respective public key and a respective private key (item 315 and 305 of

FIG. 3; Col 4, lines 43-44; The database may comprise a plurality of encrypted private keys, plurality of public keys).

- Controlling access to each user space so as to allow the sender and each recipient unrestricted access to his own user space while allowing either restricted or no access to any other user space (Col 6, lines 59-67; The server computer authenticates the hashed passphrase...the user may use his or her private key to access his or her digital messages. / the method described her is the server way of controlling Access to users information)

b. Regarding claim 2, Baltzley secure communication system discloses a virtual network connectable to a data communication network for allowing a sender to send an encrypted message to at least one recipient from any data terminal connected to the data communication network (Abstract lines 11-12 and Col 2, lines 21-25), said virtual network comprising:

- A respective public space dedicated to the user and each recipient for storing a respective public and respective private key (Col 5, lines 3-7)
- At least one computer coupled to each user space for controlling access thereto as to allow the sender and each recipient unrestricted access to his own user space for accessing his own public and private key (Col 6, lines 59-61 and item 620 of FIG. 6)
- Allowing access to the public key only in other user space (Col 6, lines 14-15 and item 625 of FIG. 6)

c. Regarding claim 3, Baltzley discloses at least one computer serves more than one user space. (Items 105 and 110 of FIG. 8)

d. Regarding claim 4, one computer is separate for each user space (items 105 and 110 of FIG. 4)

e. Regarding claim 5, the respective pubic key of the sender and of each recipient is embedded within a certificate. (Col 7, lines 61-63 and Col 1, lines 39-41; Baltzley discloses that the public keys are generally held in databases run by "Key Certificate authorities" and publicly known. Embedding the public key in a certificate requires an entity to certify the validity of the public key and to verify the recipient is who he or she claims to be, Balyzley system discloses the method for certifying the validity of public keys and their issuers)

f. Regarding claims 6 and 11, Baltzley discloses a method for sending a encrypted message by a sender to at least one recipient having a respective user space in the virtual network, the method comprising the following steps carried out by the at least one computer coupled to the senders sender's user space:

- Obtaining the respective public key of each recipient from respective user space of each recipient (Col 7, lines 2-4)
- Securely receiving the message from the data terminal, and Encrypting the message using the respective public key of each recipient (Col 7, lines 4-7)

g. Regarding claims 7, 9,13 and 15, Baltzley systems further includes:

- Conveying the encrypted message to the respective user space of each recipient to access the message from any data terminal capable of being securely receiving data from the at least one computer and being connected to the data communication network. (Col 6, lines 18-19; Col 7, lines 23-26 and items 110 and 105 of FIG. 8)

h. Regarding claims 8, 14, and 17, Baltzley further includes:

- Signing the digital message with the sender's private key (Col 6, lines 17-18)

i. Regarding claim 10, Baltzley secure communication system discloses a virtual network connectable to a data communication network for allowing a sender to send an encrypted message to at least one recipient from any data terminal connected to the data communication network (Col 2, lines 21-25), said virtual network compromises:

- A respective public space dedicated to the user and each recipient for storing a respective public and respective private key (Col 5, lines 3-7)
- At least one computer coupled to each user space for controlling access thereto as to allow the sender and each recipient unrestricted access to his own user space for accessing his own public and private key (Col 6, lines 59-61 and item 620 of FIG. 6)
- Allowing access to the public key only in other user space (Col 6, lines 14-15 and item 625 of FIG. 6)

- Database connected to the data communication network for storing respective public keys of at least a subset of users not having respective user spaces in the virtual network. (Item 805 of FIG. 8; The public key server in Baltlezy system is a repository of public keys that allows any users to query the database for a public key; Baltlezy key server fits the definition of the database storing public keys of at least subset of users not having respective user spaces in the virtual network.)

j. Regarding claim 12, Baltlzy system discloses a methods for obtaining a recipient public key comprising:

- Obtaining the respective public key of each recipient having a user space in the virtual network from the respective user space of each recipient (item 110 of FIG. 8; teaches a communication channel to communicate encrypted private key, public key and encrypted messages between internal Encryption server and clients)
- In respect of each user not having a user space in the virtual network, obtaining the respective public key of the recipient from database (item 810 of FIG. 8; teaches a communication channel to communicate encrypted private key, public key and encrypted messages between internal Encryption server and clients / item 1000 of FIG 10; teaches multiple encryption servers containing all or a subset of public keys, private keys or users information (Col 8, lines 56-59))

k. Regarding claim 16, Baltzley discloses a method for sending a encrypted message by a sender to at least one recipient having a respective user space in the virtual network, the method compromising the following steps carried out by the at least one computer coupled to the senders sender's user space:

- Obtaining the respective public key of each recipient from respective user space of each recipient (Col 7, lines 2-4)
- Securely receiving the message from the data terminal, and Encrypting the message using the respective public key of each recipient (Col 7, lines 4-7)
- Conveying the encrypted message to the respective user space of each recipient to access the message from any data terminal capable of being securely receiving data from the at least one computer and being connected to the data communication network. (Col 6, lines 18-19; Col 7, lines 23-26 and items 110 and 105 of FIG. 8)
- Baltzley system is silent on whither the user have a user a space (the user public key) in the network or not. However, this feature is deemed to be inherent to any public key cryptosystem since the sender just needs to know the recipient public key to be able to send an encrypted message; it is for this reason the public keys are known to every body. Baltzley system would be inoperative if the senders don't have access to the public keys.

l. Regarding claims 18 and 19, Baltzley discloses a computer product or program storage device readable to a respective user space dedicated to a sender and at least one recipient and storing respective public and a respective private key thereof, said program storage device tangibly embodying a program of instruction executable by the computer to perform method steps for sending an encrypted message by the sender to the at least one recipient, the method comprising the following steps:

- Obtaining the respective public key of each recipient from respective user space of each recipient (Col 7, lines 2-4)
- Securely receiving the message from the data terminal, and Encrypting the message using the respective public key of each recipient (Col 7, lines 4-7; encrypts the digital message with a client recipient public key and transmits the encrypted digital message to the encryption server)
- Conveying the encrypted message to the respective user space of each recipient to access the message from any data terminal capable of being securely receiving data from the at least one computer and being connected to the data communication network. (Col 6, lines 18-19; Col 7, lines 23-26 and items 110 and 105 of FIG. 8)

Conclusion

1. Claims 1-19 have been rejected.

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

3. Please direct all inquiries concerning this communication to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Sign Name Here

Alomari

Nov 22, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100